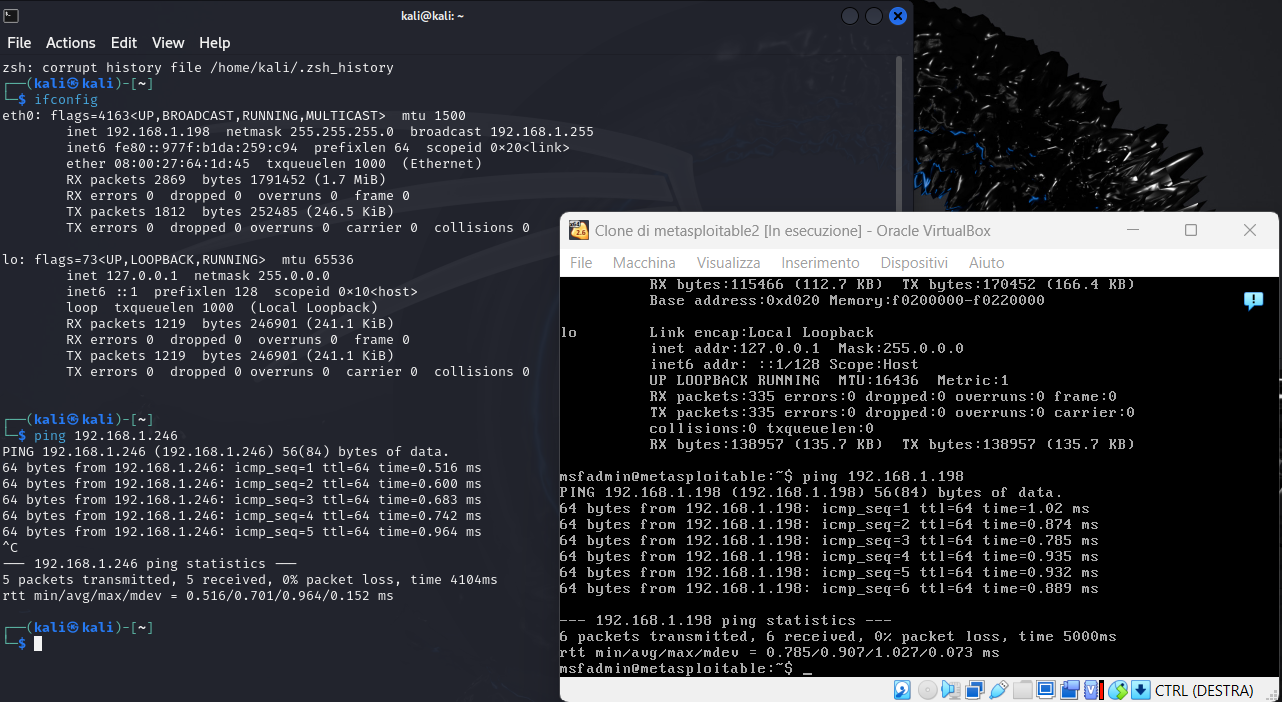
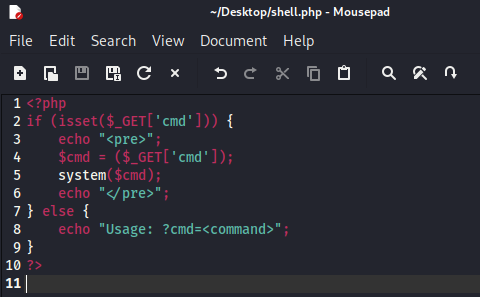
COMPITO S6L1

**Traccia:** sfruttamento di una vulnerabilità di file upload sulla DVWA per l’inserimento di una shell in php.

Come prima cosa è necessario assicurarsi che la macchina attaccante e quella bersaglio comunichino; per farlo effettuiamo un ping tra kali e metasploitable come in figura.

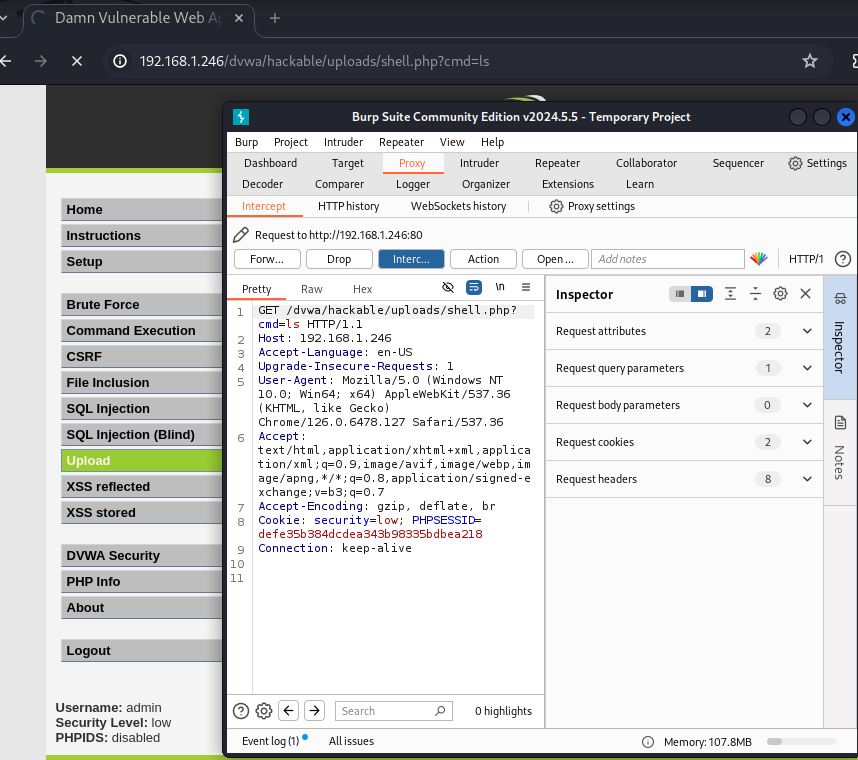
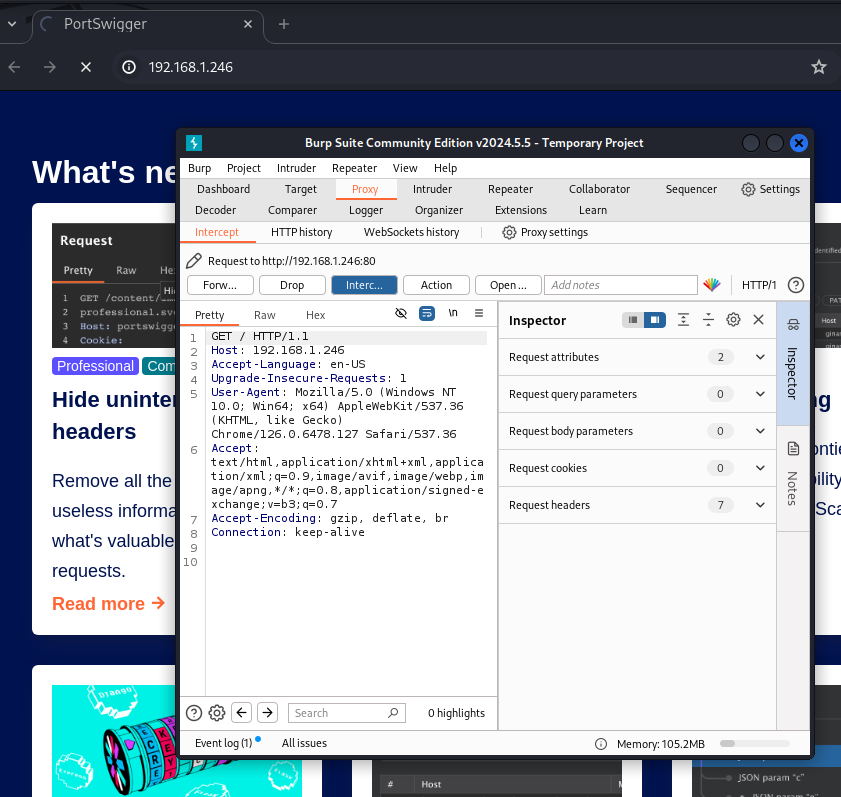
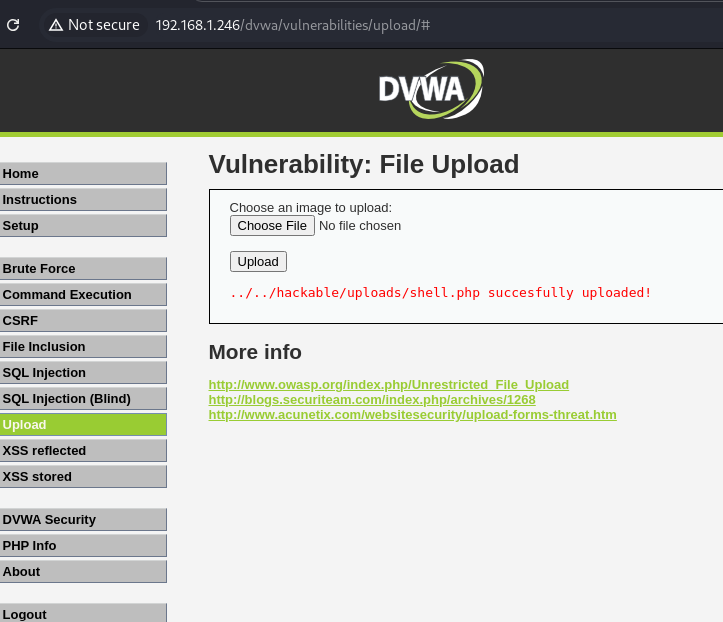


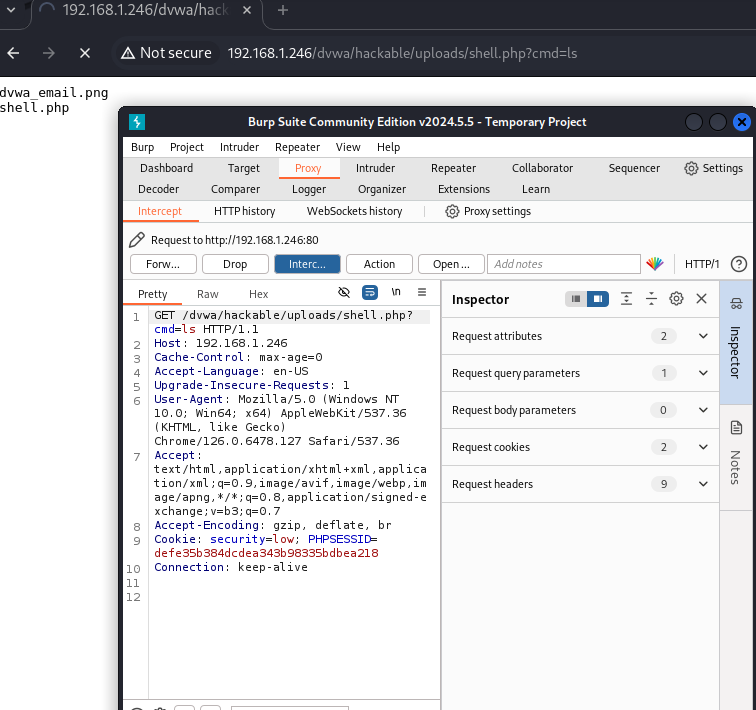
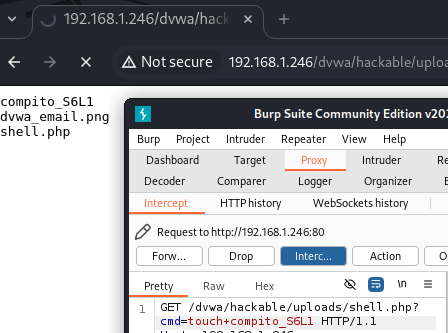
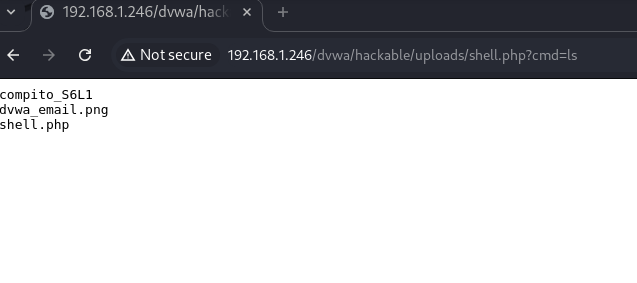
creiamo un file di testo che andremo ad importare all’interno del sito DVWA, sfruttando il metodo PUT abilitato sul sito.

Apriamo successivamente Burp Suite, che ci permetterà di visualizzare tutte le richieste che facciamo per accedere al sito DVWA, inserendo nel browser di Kali l'indirizzo IP di Metasploitable.

Ci ritroveremo quindi su DVWA dove caricheremo la shell creata in precedenza

Una volta caricato il file con successo, andremo a modificare la shell importata sfruttando il metodo PUT





Modificando il comando cmd=ls, usando il comando touch, possiamo vedere il file finale

Questa sarà invece la schermata dopo aver sfruttato il metodo PUT

Questo è ciò che ci troveremo davanti dopo aver importato la shell, ma prima di modificarla